ABSTRACT

An authentication system for mutual authentication between a terminal and a server characterized by the fact that the terminal comprises a memory means that pre-stores an authentication information P' for terminal storage; a concatenation means that yields a value P using a specific calculation formula with the input of the authentication information P' read from the memory means and a password entered for authentication; a mask operation means that yields a value Y1 using a specific calculation formula with the input of value P and an internally generated random number, and then sends Y1 to the server; and a master key generation means that yields a value MK using a specific calculation formula with the input of value P, an internally generated random number and a value Y2 received from the server, and the server comprises a memory means that pre-stores a password verification data H for server registeration; a mask operation means that yields a value Y2 using a specific calculation formula with the input of the password verification data H read from the memory means and an internally generated random number, and then sends Y2 to the terminal; and a master key generation means that yields a value MK using a specific calculation formula with the input of the password verification data H, an internally generated random number and a value Y1 received from the terminal.